proofpoint

PROOFPOINT THREAT RESPONSE

PREVENT SECURITY ALERTS AND INCIDENTS FROM ESCALATING INTO FULL-BLOWN BREACHES

BENEFITS OF THREAT RESPONSE

- Automate collection of forensic data from potentially compromised systems
- Save countless hours confirming infections by comparing system PC data with detection forensics
- Reduce manual collection of data from external devices, intelligence sources and more
- Monitor incidents and processed threats with a visual interface that lets you see what's happening at a glance
- Accelerate response decisions with integrated views of threat activity
- Quarantine and contain threats automatically or at the push of a button for fast protection
- Automatically manage users, emails, hosts, IPs, and URLs on enforcement systems throughout the attack lifecycle to free up staff for other tasks
- Get an auditable history of response actions to boost the ROI of your existing infrastructure
- Reduce dependency on custom-coded software
- Automatically create, track, and manage incident records to reduce the need for manual entry
- Stay current on malicious activity with up-to-the-minute reports of targeted users, systems, groups, and departments

Proofpoint Threat Response™ is a force multiplier for security operations that orchestrates and automates incident response. The platform surrounds security alerts with rich contextual data to help security teams prioritise and execute response actions. It collects and analyses security event context around incidents and investigations, and it collects endpoint forensics to confirm system infections to create actionable profiles of incidents. Based upon the enhanced context, it enables enforcement and quarantine actions automatically or at the push of a button leveraging existing infrastructure.

MANUAL RESPONSE DOESN'T SCALE

At many organisations, security incident response is a slow, labor-intensive process. Time-intensive tasks turn into painful bottlenecks, including:

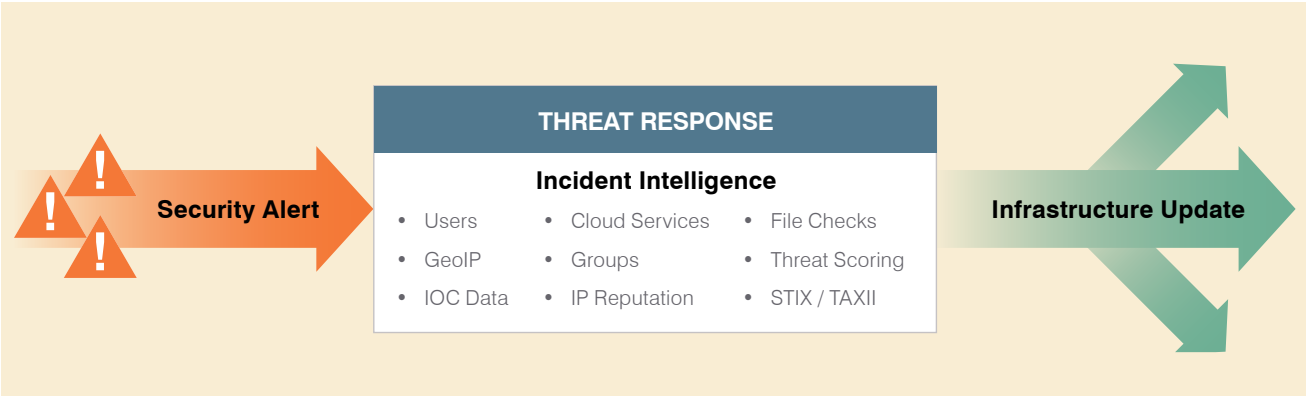
- Identifying high-value targets to prioritise threats
- Identifying high-value threats that may be part of larger campaigns or botnets
- Collecting and comparing endpoint forensics for signs of infection
- Managing investigations that may span multiple targets and alerts
- Negotiating between security and infrastructure with implementation time for enforcement

Repeating these tasks for every incident can overwhelm already stretched security teams, resulting in skipped steps and cut corners.

The Incident Investigation Time Penalty

Incident response investigation requires information from multiple disconnected sources where each additional data point is like a piece of a puzzle. As each piece is added, organised and analysed, scope, severity, and priority become clearer.

Confirming that a system has been compromised usually requires a series of manual, time-consuming steps. During the investigation phase, valuable data may be stolen from infected systems while attackers may be moving laterally across the network. The quest for a complete investigation often comes at the cost of putting data at risk.



MODERNISE INCIDENT RESPONSE WITH THREAT RESPONSE

Threat Alert Source Collection and Investigation

Incident response has four main areas of focus:

- Investigate the "who, what, and where" of attacks, including targeted users, systems, and campaigns
- Verify targeted system forensics against sandbox forensic reports
- Stop the bleeding and IP loss with quarantine and containment actions
- Track incident response KPIs to ensure incidents are not missed or forgotten

These focus areas help identify which users are infected and the severity and urgency of a threat. It also helps eliminate false positives and stop the infections from spreading and data from being exfiltrated.

Who, What, and Where with Threat Response

You need to immediately determine which internal users, departments, and groups are affected. Knowing "who" means you can prioritise high-value targets such as the CFO, executive staff and finance systems over the mailroom or lower priority targets.

Besides internal context and intelligence, external factors can provide clues to suspicious IPs or domains in security alerts. These factors are pre-integrated into Threat Response with the ability to import and leverage 3rd party intelligence, including STIX/TAXII feeds, to further automate analysis.

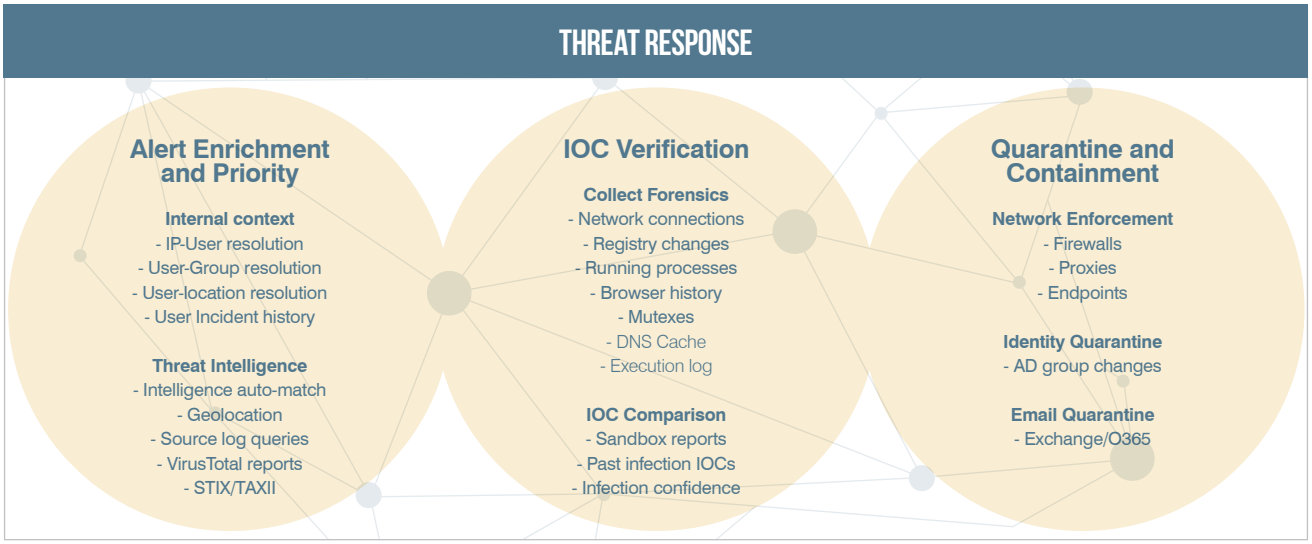
These key external factors include:

- Domain freshness/length of registration
- Domain blacklisting
- IP and URL reputation (category and history)
- IP geolocation
- Associated campaigns
- Targeted industries for categories of customers

Infection Confirmation by Automatic IOC Verification

Threat Response collects and analyses endpoint forensics from targeted systems to yield a rich snapshot of indicators of compromise (IOC). IOC data includes the following:

- Registry changes
- File changes
- Recent file execution log events
- Mutexes
- Network connections
- File deletion log events
- Running processes
- Browser history
- DNS Cache



This information is compared to changes reported by malware analysis tools and other systems to provide insight into the health of the client. In addition, user designed Powershell scripts can also be pushed endpoints for custom data collection or other activities.

Another key capability is checking attacked systems for past infections. When Threat Response performs an on-demand endpoint collection, it checks for IOCs not only from the current attack, but from past infections seen in your environment. This approach helps quickly and effectively verify whether past infections have spread to the system being targeted now.

Out-of-the-Box Integration with Premium Intelligence and Third-Party Tools

Threat Response automatically checks every domain and IP provided in security alerts and sandbox reports against its built-in premium intelligence feeds, including Emerging Threats Intelligence. This step removes hours of tedious work and manual one-by-one searching against intelligence services to find attacking IPs and hosts leveraging known bad sites.

Threat Response can automatically or manually import threat intelligence from third parties via STIX and TAXII. This means that security teams can import and automatically match against threat feeds from various Information sharing and analysis centers (ISACs) out of the box. It supports other “bring your own intelligence” datasets via upload or by manually adding intelligence.

Using built-in VirusTotal integration, files can be checked not only once, but over time. You can see how many of 50+ anti-virus engines detect malicious signatures or properties in files dropped, downloaded or unpacked during a potential infection. Other out-of-the-box integrations include WHOIS lookups, geolocation, Active Directory connectors, and more.

Quarantine and Containment

Based-on the context and forensics collected and analysed by the system, Threat Response presents a context rich view of the threat. This view allows analysts to take push-button response actions, identify, areas for additional investigation, or turn on automated response such as retract delivered email from users’ mailboxes, add users to low permission groups, or update blocklists of firewalls and web filters.

Incident management

A hidden risk of incident handling is the loss of context due to the amount of system consoles and browser tabs used in combination with the copy and pasting of information between those systems. In addition to the core capabilities, Threat Response includes key incident management functions that enable users and teams to investigate incidents without losing that context while jumping from system to system. Beyond the basics of

assignment and assignment tracking Threat Response also:

- Maintains a history and record for every incident and every action taken
- Tracks incident assignments at the individual and team levels
- Combines incidents into investigations
- Enables users or team members to operate at different permissions
- Triggers workflow notifications as incidents progress and change status
- Honors roles and permissions for quarantine actions, insuring only the right people can take actions at the right time
- Notifies users or teams when incidents change, such as when threat scores pass a threshold or when a quarantine action has completed

BENEFITS

Example benefits from using Threat Response and automating quarantine and contain actions include:

- Adding Database admins to a restricted penalty box, blocking access to sensitive information during an incident
- Clawing back delivered email to eliminate the risk of users clicking on malicious URLs or attachments again
- Blocking communication from all employees to CNC sites to break the control chain
- Limiting the ability for malware infections to spread to other systems
- Reducing redundant or duplicate analyst work by understanding larger investigations of campaigns hitting your organisation
- Visualising KPIs around slow or unprocessed incidents, incident handling throughput, and targeting of departments or permissioned groups
- Installation and setup in hours means increased security and response handling results and rapid ROI

SUMMARY

Threat Response is a force multiplier for incident response. It delivers security orchestration and automation out-of-the-box by wrapping context, forensic collection and IOC comparison for infection verification, quarantine and containment capabilities, and incident management features around incidents and investigations.

OUT-OF-THE-BOX INTEGRATIONS

ALERT SOURCE

- Cisco FirePOWER NGIPS
- FireEye EX Series
- FireEye NX Series
- HP ArcSight ESM
- IBM QRadar
- JSON Event Source
- Juniper Secure Analytics
- Palo Alto Networks Wildfire
- Proofpoint TAP
- Splunk Enterprise
- Suricata

CUSTOM RESPONSE

- JSON Custom response API

EIDR

- Tanium
- Carbon Black

EMAIL QUARANTINE

- Microsoft Exchange

ENFORCEMENT DEVICE

- Check Point
- Cisco ASA
- Cisco IOS
- Cisco OpenDNS
- CyberArk Enterprise Vault
- Fortinet FortiGate
- Imperva SecureSphere
- Juniper SRX (JUNOS)
- Palo Alto Networks NGFW
- Palo Alto Networks Panorama

ENRICHMENT

- Emerging Threats
- MaxMind
- Microsoft Active Directory
- Proofpoint Threat Graph
- Soltra
- Splunk Enterprise
- Virus Total
- WHOIS

IDENTITY ACCESS MANAGEMENT

- Centrify
- Microsoft Azure SSO
- Okta
- OneLogin
- Ping Identity

PROXY, DYNAMIC BLOCK LISTS

- Blue Coat ProxySG
- Palo Alto Networks NGFW

TICKETING

- BMC Remedy Ticketing System
- JIRA

TWO FACTOR AUTHENTICATION SOLUTIONS

- Duo Security
- RSA Securid
- SafeNet
- Symantec 2FA

ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organisations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organisations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.